

PCT/JP99/05704

4
日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

15.10.99	
REC'D 29 OCT 1999	
WIPO	PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

1998年10月15日

出願番号
Application Number:

平成10年特許願第309418号

出願人
Applicant(s):

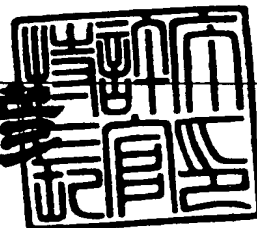
三菱商事株式会社

PRIORITY
DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

1999年10月 1日

特許庁長官
Commissioner,
Patent Office

近藤隆彦



出証番号 出証特平11-30670

BEST AVAILABLE COPY

【書類名】 特許願

【整理番号】 S98033

【提出日】 平成10年10月15日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/00

【発明の名称】 2重再暗号化によりデジタルデータを保護する方法及び装置

【請求項の数】 8

【発明者】

【住所又は居所】 東京都多摩市貝取2-12-6-104

【氏名】 斉藤 誠

【特許出願人】

【識別番号】 000005979

【住所又は居所】 東京都千代田区丸の内二丁目6番3号

【氏名又は名称】 三菱商事株式会社

【代理人】

【識別番号】 100099379

【弁理士】

【氏名又は名称】 南條 眞一郎

【手数料の表示】

【予納台帳番号】 027982

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【書類名】 明細書

【発明の名称】 2重再暗号化によりデジタルデータを保護する方法及び装置

【特許請求の範囲】

【請求項1】 暗号化デジタルデータを復号化し、復号化されたデジタルデータを利用するとともに、復号化された前記デジタルデータを外部の可変鍵を用いて再暗号化し、再暗号化された前記デジタルデータを内部の固定鍵を用いて2重に再暗号化し、2重に再暗号化された前記デジタルデータを保存あるいは転送し、保存あるいは転送された2重に再暗号化された前記デジタルデータを前記内部の固定鍵をもちいて再復号化し、再復号化された前記デジタルデータを前記外部の可変鍵を用いて2重に再復号化して利用する、デジタルデータ保護方法。

【請求項2】 暗号化デジタルデータを復号化し、復号化されたデジタルデータを利用するとともに、復号化された前記デジタルデータを内部の固定鍵を用いて再暗号化し、再暗号化された前記デジタルデータを内部の可変鍵を用いて2重に再暗号化し、2重に再暗号化された前記デジタルデータを保存あるいは転送し、保存あるいは転送された2重に再暗号化された前記デジタルデータを前記外部の可変鍵をもちいて再復号化し、再復号化された前記デジタルデータを前記内部の固定鍵を用いて2重に再復号化して利用する、デジタルデータ保護方法。

【請求項3】 外部の可変鍵を用いての再暗号化及び再復号化がソフトウェアによって行われる請求項1又は2のデジタルデータ保護方法。

【請求項4】 外部の可変鍵を用いての再暗号化及び再復号化がハードウェアによって行われる請求項1又は2のデジタルデータ保護方法。

【請求項5】 暗号化デジタルデータを復号化し、復号化されたデジタルデータを利用するとともに、復号化された前記デジタルデータを外部の可変鍵を用いて再暗号化し、再暗号化された前記デジタルデータを内部の固定鍵を用いて2重に再暗号化し、2重に再暗号化された前記デジタルデータを保存あるいは転送し、保存あるいは転送された2重に再暗号化された前記デジタルデータを前記内部の固定鍵をもちいて再復号化し、再復号化された前記デジタルデータを前記外部の可変鍵を用いて2重に再復号化して利用する、デジタルデータ保護装置。

【請求項6】 暗号化デジタルデータを復号化し、復号化されたデジタルデー

タを利用するとともに、復号化された前記デジタルデータを内部の固定鍵を用いて再暗号化し、再暗号化された前記デジタルデータを内部の可変鍵を用いて2重に再暗号化し、2重に再暗号化された前記デジタルデータを保存あるいは転送し、保存あるいは転送された2重に再暗号化された前記デジタルデータを前記外部の可変鍵をもちいて再復号化し、再復号化された前記デジタルデータを前記内部の固定鍵を用いて2重に再復号化して利用する、デジタルデータ保護装置。

【請求項7】 外部の可変鍵を用いての再暗号化及び再復号化がソフトウェアによって行われる請求項1又は2のデジタルデータ保護方法。

【請求項8】 外部の可変鍵を用いての再暗号化及び再復号化がハードウェアによって行われる請求項1又は2のデジタルデータ保護方法。

【発明の詳細な説明】

【0001】

【利用分野】

本発明は、デジタルコンテンツの管理、特に著作権主張がされたデジタルコンテンツの著作権管理、デジタルコンテンツの秘密保護、を行うシステムに関する。

【0002】

【従来技術】

従来広く普及しているアナログコンテンツは保存、複写、加工、転送をする毎に品質が劣化するために、これらの作業によって生じる著作権の処理は大きな問題とはならなかった。しかし、デジタルコンテンツは保存、複写、加工、転送を繰り返して行っても品質劣化が生じないため、これらの作業によって生じる著作権の処理は大きな問題である。

【0003】

デジタル映像・音声等のデジタルデータは放送、DVD等によって有料でユーザに供給されることが多く、その場合に無料視聴を防止するために暗号化されて供給される。暗号化されて供給されたデジタルデータは何等かの手段によって供給された暗号鍵を用いて復号され、視聴される。復号されたデジタルデータは保存、複写あるいは転送を行っても品質が劣化することはないため、ユーザによっ

て保存、複写あるいは転送が行われた場合には二次的な無料視聴が行われることになり、復号されたデジタルデータコンテンツの再度の利用はコンテンツ提供者の利益に反するため、再度の利用すなわち保存、複写あるいは転送の二次利用を禁止することでシステム及び機器の開発が進められてきた。

【0004】

しかし、二次利用を禁止することは利用者にとってはデジタルデータコンテンツの利用が魅力の乏しいものとなり、デジタルデータコンテンツの普及を阻害する要因となりかねないことが認識され、復号されたデジタルデータコンテンツの再暗号化を行うことにより不法な利用を防止するとともに、利用者にとってデジタルデータコンテンツの利用が十分に魅力あるものにすることが提案されている。

【0005】

媒体に格納されてユーザに譲渡あるいは貸与されたデジタルデータ及びユーザに転送されたデジタルデータの保存・複写あるいは転送等の二次利用における著作権の保護は、デジタルデータがユーザの手許にあるためデジタルデータの著作権者が自ら行うことは不可能であり、何らかの方法により自動的かつ強制的に行う必要がある。

【0006】

このような状況に鑑みて、本発明者はこれまでにデジタルコンテンツの著作権を保護することを目的としてこれまでに様々な提案を行ってきた。

本発明者らは特開平6-46419号及び特開平6-1410004号で公衆電信電話回線を通じて鍵管理センタから許可鍵を入手することによって著作権管理を行うシステムを、特開平6-132916号でそのための装置を提案した。

【0007】

また、特開平7-271865号及び特開平8-185448号において、デジタルコンテンツの著作権を管理するシステムについて提案した。

【0008】

これらのシステム及び装置において、暗号化された番組の視聴を希望する者は通信装置を使用し通信回線を経由して管理センタに視聴申し込みを行い、管理セ

ンタはこの視聴申し込みに対して許可鍵を送信するとともに課金処理を行い料金を徴収する。

許可鍵を受信した視聴希望者はオンラインあるいはオフライン手段によって許可鍵を受信装置に送り込み、許可鍵を送り込まれた受信装置はその許可鍵によって暗号化された番組の暗号を解除する。

【0009】

特開平7-271865号に記載されたシステムは、デジタル映像コンテンツのリアルタイム送信も含むデータベースシステムにおけるデジタルコンテンツの表示（音声化を含む）、保存、複写、加工、転送における著作権の管理を行うために、利用を許可する鍵の他に、著作権を管理するためのプログラム及び著作権情報を用いる。この著作権管理プログラムは、申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【0010】

また、この特開平7-271865号には、デジタルコンテンツが暗号化された状態でデータベースから供給され、著作権管理プログラムによって表示・加工のときにのみ復号化され、保存、コピー、転送は再び暗号化された状態で行うことが記載されている。さらに、著作権管理プログラム自体を暗号化し、許可鍵で著作権管理プログラムを復号化し、復号化された著作権管理プログラムが著作権データの復号化及び暗号化を行うこと、データの保存及び表示以外の利用が行われた場合には操作者についての情報を含む著作権情報を原著作権情報に加えて履歴として保存することも記載されている。

【0011】

特開平8-287014号において著作権管理を行うためのボード、PCMCIAカードあるいはICカードの形態を有する復号／再暗号化用装置及び暗号鍵の寄託システムを提案した。またこの出願では著作権管理方法のテレビジョン会議及び電子商取引への応用についても言及した。

【0012】

特開平8-272745号において複数データを利用した加工データの原データ著作権及び加工データ著作権の保護を秘密鍵方式と公開鍵方式を組み合わせ

加工プログラムへのデジタル署名で申込みの正当性を確認することによって行うシステムを提案した。

【0013】

特開平8-288940号において、データベース、ビデオオンデマンド（VOD）システムあるいは電子商取引に著作権管理システムを適用するための様々の形態を提案した。

【0014】

特開平8-329011号において、複数データを利用・加工する場合の原データ及び新データの著作権保護を第三の暗号鍵及び著作権ラベルを用いて行うシステムを提案した。

【0015】

以上説明した本発明者が提案してきたデータ著作権管理システム及びデータ著作権管理装置から理解されるように、データ著作権の管理は著作権管理プログラムによって暗号化／復号化／再暗号化及び利用内容の制限を行うことによって実現される。この暗号技術及び利用制限はコンピュータを使用することによって実現される。

【0016】

さらに、ネットワークを経由して秘密情報を交換する場合には窃取防止のために情報の暗号化が行われる。

伝送時の情報窃取を暗号化により防止することが、USP 5504818, 515441に述べられており、その場合に複数の暗号鍵を用いることがUSP 5504816, 5353351, 5475757及び5381480に述べられており、再暗号化を行うことがUSP 5479514に述べられている。

【0017】

著作権管理プログラムによるデジタルデータの二次利用における著作権の保護は、復号されたデジタルデータの再暗号化／再復号化とこの再暗号化／再復号化を著作権管理プログラムによって管理・実行することによって実現される。

いうまでもなく、再暗号化／再復号化を行う手段としてソフトウェアウェアによるものとハードウェアによるものがある。

【0018】

非暗号化データMを暗号鍵Kを用いて暗号化データCを得ることは、

$$C = E(M, K)$$

という式で表現され、暗号化データCを暗号鍵Kを用いて復号化データMを得ることは、

$$M = D(C, K)$$

という式で表現される。

【0019】

また、復号化データMの再暗号化／再復号化を繰り返す場合の再暗号化は、

$$C_i = E(D(C_{i-1}, K_{i-1}), K_i) \quad \text{但し } i \text{ は正の整数}$$

という式で表現され、再復号化は、

$$M = D(E(C_{i-1}, K_{i-1}), K_i)$$

という式で表現される。

【0020】

図1により、従来提案されているセットトップボックス(STB)の構成及びこのセットトップボックスで行われているデジタルデータ保護方法を説明する。

なお、暗号化／復号化と直接には関係がない周辺回路、例えば増幅ユニット、圧縮／伸長ユニットはこの説明において省略されている。

【0021】

この図において、1はデジタル地上波放送、デジタルCATV放送、デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいはDVD、CD等のデジタル保存媒体により供給されるデジタルデータであり、不正利用を防止するために暗号鍵K1を用いて暗号化されて、

$$C1 = E(M, K1)$$

セットトップボックス2に供給される。

【0022】

暗号化デジタルデータC1を供給されたセットトップボックス2では、暗号化デジタルデータC1と同じ経路あるいは暗号化デジタルデータC1と異なる経路により鍵センターから入手した暗号鍵K1を用い、復号化ユニット3において暗号

化デジタルデータC1を復号し、

$$M = D(C1, K1)$$

復号化データMがディスプレイ装置4等に出力される。

【0023】

復号化データMがデジタルビデオディスクRAM(DVD)あるいはハードディスク等の媒体に保存される場合、又はネットワークを経由して外部に転送される場合は、内蔵固定鍵方式暗号化／復号化ユニット5の再暗号化ユニット6において復号化データMがその内蔵固定鍵方式暗号化／復号化ユニット5に内蔵された固定暗号鍵K0を用いて再暗号化され、

$$C0 = E(M, K0) = E(D(C1, K1), K0)$$

再暗号化データC0として外部装置8に保存あるいは転送される。

【0024】

再暗号化データC0が再利用される場合には、外部装置8の保存媒体から読み出されたあるいはネットワークを経由して転送された再暗号化データC0が内蔵固定鍵方式暗号化／復号化ユニット5の再復号化ユニット7においてその内蔵固定鍵方式暗号化／復号化ユニット5に内蔵された固定暗号鍵K0を用いて再復号化され、

$$M = D(C0, K0) = D(E(D(C1, K1), K0), K0)$$

復号化データMがディスプレイ装置4等に出力される。

なお、この場合安全を期するために、図中に破線で示した経路により再暗号化データC0が保存媒体から読み出される時に保存媒体中の再暗号化データC0が消去され、再度内蔵固定暗号鍵K0を用いて再暗号化されたものが再保存されるように構成されることもある。

なお、米国特許5805706号には再暗号化／再復号化を行う集積回路が示されている。

【0025】

このように構成されたセットトップボックスは、再暗号／再復号がハードウェアにより内蔵固定鍵K0を用いて自動的に行われるため取り扱いが容易であり、保護する必要のあるデジタルデータの強制的再暗号／再復号化には有効である。

しかし、暗号鍵K0が装置に内蔵かつ固定されているため、暗号鍵K0が知られてしまう恐れがあり、その場合には以後そのデジタルデータの保護は不可能になる。

【0026】

【発明の概要】

この問題を解決するために、本出願では内蔵固定鍵を用いる再暗号化に加えて外部の可変鍵を用いて2重に再暗号化する方法及び装置の発明を提供する。

内蔵固定鍵と外部可変鍵の使用順には、初めに可変鍵を用い次に固定鍵を用いる場合と、初めに固定鍵を用い次に可変鍵を用いる場合とがある。

【0027】

初めに再暗号化に用いられた鍵は後の復号化に用いられるため、後で行われた再暗号が解読された場合でも、解読に対する耐性は高い。したがって、初めに外部可変鍵を用い次に内蔵固定鍵を用いて再暗号化した場合には内蔵固定鍵が知られてしまった場合でも外部固定鍵が知られる可能性は著しく低い。

【0028】

実施形態としてはソフトウェアによる場合とハードウェアによる場合があり、さらにソフトウェアとハードウェアの組み合わせがある。ハードウェアとしてはデジタルビデオに向けて開発された内蔵固定鍵を用いるハードウェアが利用可能である。

【0029】

ソフトウェアによる場合プログラム及び使用される鍵の安全性を保全するためにユーザが利用することができないカーネル部以下の領域で暗号化／復号化を行う。具体的にはI/Oマネージャ内のフィルタドライバ、ディスクドライバ・ネットワークドライバであるデバイスドライバ、HALを利用するリアルタイムOSで暗号化／復号化を行う。フィルタドライバはファイルシステムドライバを挟んで2つあるがどちらも利用可能であり、さらには両方を利用することも可能である。

【0030】

【実施例】

本願発明の実施例を説明する。

図2により本発明を適用した第1実施例であるセットトップボックス（STB）の構成及びこのセットトップボックスで行われているデジタルデータ保護方法を説明する。

なお、この実施例のセットトップボックスにおいても図1に示された従来例のセットトップボックスの場合と同様に、暗号化／復号化と直接には関係がない周辺回路、例えば増幅ユニット、圧縮／伸長ユニットの説明は省略されている。

【0031】

この実施例が図1に示された従来提案されているセットトップボックスと大きく異なる点は、復号化ユニット13と内蔵された固定鍵K0を用いて暗号化／復号化を行う内蔵固定鍵方式暗号化／復号化ユニット15の間にセットトップボックスの外部から供給された可変鍵K2を用いて暗号化／復号化を行う外部可変鍵方式暗号化／復号化ユニット19が挿入されている点である。

【0032】

この図において、11はデジタル地上波放送、デジタルCATV放送、デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいはDVD、CD等のデジタル保存媒体により供給されるデジタルデータであり、不正利用を防止するために暗号鍵K1を用いて暗号化されて、

$$C1 = E(M, K1)$$

セットトップボックス12に供給される。

【0033】

暗号化デジタルデータC1を供給されたセットトップボックス12では、暗号化デジタルデータC1と同じ経路あるいは暗号化デジタルデータC1と異なる経路により鍵センタから入手した暗号鍵K1を用い、復号化ユニット13において暗号化デジタルデータC1を復号し、

$$M = D(C1, K1)$$

復号化データMがディスプレイ装置14等に出力される。

【0034】

著作権主張がなされた復号化データMが外部装置18であるデジタルビデオデ

ディスク (DVD) RAMあるいはハードディスク等の媒体に保存される場合、又はネットワークを経由して外部に転送される場合は、暗号化デジタルデータC1と同じ経路あるいは暗号化デジタルデータC1と異なる経路を経由して入手した外部可変鍵K2を用い、外部可変鍵方式暗号化／復号化ユニット19の再暗号化ユニット20において復号化データMが強制的に再暗号化され、

$$C2 = E(M, K2) = E(D(C1, K1), K2)$$

さらに内蔵固定鍵方式暗号化／復号化ユニット15の再再暗号化ユニット16において再暗号化データC2がその内蔵固定鍵方式暗号化／復号化ユニット15に内蔵された固定暗号鍵K0を用いて再再暗号化され、

$$C2-0 = E(C2, K0) = E(E(D(C1, K1), K2), K0)$$

再再暗号化データC2-0として外部装置18に保存あるいは転送される。

【0035】

再再暗号化データC2-0が再利用される場合には、外部装置18の保存媒体から読み出されたあるいはネットワークを経由して転送された再暗号化データC2-0が内蔵固定鍵方式暗号化／復号化ユニット15の再復号化ユニット17において内蔵固定鍵方式暗号化／復号化ユニット15に内蔵された固定暗号鍵K0を用いて再復号化され、

$$C2 = E(C2-0, K0) = D(E(E(D(C1, K1), K2), K0)$$

さらに外部可変鍵方式暗号化／復号化ユニット19の再再復号化ユニット21において再復号化データC2が暗号化デジタルデータC1と同じ経路あるいは暗号化デジタルデータC1と異なる経路により鍵センターから入手した外部可変鍵K2を用いて復号化され、

$$M = D(C2, K2) = D(E(D(C1, K1), K2)$$

復号化データMがディスプレイ装置14等に出力される。

【0036】

なお、この場合安全を期するために、図中に破線で示した経路により再暗号化データC2-0が保存媒体から読み出される時に保存媒体中の再暗号化データC2-0が消去され、外部可変鍵K2及び内蔵固定暗号鍵K0を用いて再暗号化されたものが再保存されるように構成されることもある。

【0037】

このように、内蔵固定鍵を用いて再暗号化する前に外部可変鍵を用いて再暗号化する構成により、万一内蔵固定鍵が知られてしまった場合でもデータは外部可変鍵でも暗号化されているため、さらに外部可変鍵を見いだして暗号化データの解読を行うことは極めて困難になる。

【0038】

また、外部可変鍵は初めに使用され、内蔵固定鍵が使用された後に、最後に使用されるため、暗号鍵の安全性が高く、かつ初めに使用されることにより、暗号化データを最も強力に支配することになる。

【0039】

この実施例においては、再暗号化ユニット20及び再再復号化ユニット21が外部可変鍵方式暗号化／復号化ユニット19に含まれ、再再暗号化ユニット16及び再暗号化ユニット17が内蔵固定鍵方式暗号化／復号化ユニット15に含まれたものについて説明したが、これらのユニット16、17、20、21が分離して設けられても良いことは当然のことである。

【0040】

図3により本発明を適用した第2実施例であるセットトップボックス（STB）の他の構成及びこのセットトップボックスで行われているデジタルデータ保護方法を説明する。

【0041】

なお、この第2実施例のセットトップボックスにおいても図1に示された従来例のセットトップボックスの場合と同様に、暗号化／復号化と直接には関係がない周辺回路、例えば増幅ユニット、圧縮／伸長ユニットの説明は省略されている。

【0042】

この第2実施例のセットトップボックスが図2に示された第1実施例のセットトップボックスと異なる点は、内蔵された固定鍵K0を用いて暗号化／復号化を行う内蔵固定鍵方式暗号化／復号化ユニット35とセットトップボックスの外部から供給された可変鍵K2を用いて暗号化／復号化を行う外部可変鍵方式暗号化

／復号化ユニット 39 の挿入位置が入れ替わっている点である。

すなわち、復号化ユニット 33 に内蔵された固定鍵 K_0 を用いて暗号化／復号化を行う内蔵固定鍵方式暗号化／復号化ユニット 35 が配置され、外部可変鍵 K_2 を用いて暗号化／復号化を行う外部可変鍵方式暗号化／復号化ユニット 39 が配置されている点である。

【0043】

この図において、31 はデジタル地上波放送、デジタルCATV放送、デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいはDVD、CD等のデジタル保存媒体により供給されるデジタルデータであり、不正利用を防止するために暗号鍵 K_1 を用いて暗号化されて、

$$C1 = E(M, K1)$$

セットトップボックス 32 に供給される。

【0044】

暗号化デジタルデータ $C1$ を供給されたセットトップボックス 32 では、暗号化デジタルデータ $C1$ と同じ経路あるいは暗号化デジタルデータ $C1$ と異なる経路により鍵センタから入手した暗号鍵 K_1 を用い、復号化ユニット 33 において暗号化デジタルデータ $C1$ を復号し、

$$M = D(C1, K1)$$

復号化データ M がディスプレイ装置 34 等に出力される。

【0045】

著作権主張がなされた復号化データ M が外部装置 38 であるデジタルビデオディスク (DVD) RAM あるいはハードディスク等の媒体に保存される場合、又はネットワークを経由して外部に転送される場合は、内蔵固定鍵方式暗号化／復号化ユニット 35 の再暗号化ユニット 36 において再暗号化データ $C2$ がその内蔵固定鍵方式暗号化／復号化ユニット 35 に内蔵された固定暗号鍵 K_0 を用いて再再暗号化され、

$$C0 = E(M, K0) = E(D(C1, K1), K0)$$

さらに暗号化デジタルデータ $C1$ と同じ経路あるいは暗号化デジタルデータ $C1$ と異なる経路を経由して入手した外部可変鍵 K_2 を用い、外部可変鍵方式暗号化／

復号化ユニット 39 の再再暗号化ユニット 40 において復号化データ M が強制的に再再暗号化され、

$$C0-2 = E(C0, K2) = E(E(D(C1, K1), K0), K2)$$

再再暗号化データ C0-2 として外部装置 38 に保存あるいは転送される。

【0046】

再再暗号化データ C0-2 が再利用される場合には、外部装置 38 の保存媒体から読み出されたあるいはネットワークを経由して転送された再暗号化データ C0-2 が外部可変鍵方式暗号化／復号化ユニット 39 の再復号化ユニット 41 において外部可変鍵 K2 を用いて再復号化され、

$$C0 = E(C0-2, K2) = D(E(E(D(C1, K1), K0), K2))$$

さらに内蔵固定鍵方式暗号化／復号化ユニット 35 の再再復号化ユニット 37 において再復号化データ C2 が内蔵固定鍵方式暗号化／復号化ユニット 35 に内蔵された固定暗号鍵 K0 を用いて再再復号化され、

$$M = D(C0, K0) = D(E(D(C1, K1), K0))$$

復号化データ M がディスプレイ装置 34 等に出力される。

【0047】

なお、この場合安全を期するために、図中に破線で示した経路により再暗号化データ C0-2 が保存媒体から読み出される時に保存媒体中の再再暗号化データ C0-2 が消去され、内蔵固定暗号鍵 K0 及び外部可変鍵 K2 を用いて再暗号化されたものが再保存されるように構成されることもある。

【0048】

このように、内蔵固定鍵を用いて再暗号化する前に外部可変鍵を用いて再暗号化する構成により、もし内蔵固定鍵が知られてしまった場合でもデータは外部可変鍵でも暗号化されているため、さらに外部可変鍵を見いだして暗号化データの解読を行うことは極めて困難になる。

【0049】

また、この構成は図 1 に示された従来提案されているセットトップボックスの内蔵固定鍵方式暗号化／復号化ユニット 35 にさらに外部可変鍵方式暗号化／復号化ユニット 41 を単純に付加した構成であるから、セットトップボックスの設

計が容易である。

【0050】

この実施例においては、再暗号化ユニット36及び再再復号化ユニット37が内蔵固定鍵方式暗号化／復号化ユニット35に含まれ、再再暗号化ユニット40及び再暗号化ユニット41が外部可変鍵方式暗号化／復号化ユニット39に含まれたものについて説明したが、これらのユニット36、37、40、41が分離して設けられても良いことは当然のことである。

【0051】

デジタルデータコンテンツの取り扱いはセットトップボックスで行われるばかりでなく、パーソナルコンピュータ等のコンピュータでも行われる。

図4にから図7により、パーソナルコンピュータを用いた装置に適用した本発明の実施例を説明する。

【0052】

パーソナルコンピュータはセットトップボックスのように全てがハードウェアで構成されハードウェアのみによって動作する装置とは異なり、装置に内蔵されたハードウェアをソフトウェアを用いて制御することによって動作する装置である。

【0053】

コンピュータを効率的に使用するために、コンピュータの全体の動作を統括するオペレーティングシステム(OS)が用いられている。

パーソナルコンピュータ等で使用されている従来のオペレーティングシステムはメモリ管理、タスク管理、割り込み、プロセス間通信という基本的なサービスを扱うカーネル(Kernel)と、その他のサービスを扱うオペレーティングシステムサービスで構成されていた。

【0054】

しかしながら、マイクロプロセッサの能力向上、主記憶装置として使用されるRAM価格の低下というコンピュータ側の情勢変化と、コンピュータに対する利用者からの要求性能の向上に伴い、コンピュータの全体の動作を統括するオペレーティングシステムも機能向上が要求され、以前と比較してオペレーティングシ

システムの規模が肥大している。

【0055】

このような肥大したオペレーティングシステムはオペレーティングシステム自身がその保存場所であるハードディスクの大きなスペースを占領するため、ユーザが必要とするアプリケーションプログラムあるいはデータを保存するスペースが不足がちになり、コンピュータの使い勝手が悪くなるという事態が発生する。

【0056】

このような事態に対処するために、最新のオペレーティングシステムはカーネルから他のオペレーティングシステムのエミュレーション及び画面描画を行う環境サブシステムと、セキュリティサブシステム等の中核サブシステムとをユーザに依存する部分であるサブシステム(Sub system)として取り除き、ハードウェアの相異を吸収するHAL(Hardware abstraction Layer)、スケジューリング機能、割り込み機能、I/O管理機能等の基本的部分をマイクロカーネル(Micro kernel)とし、サブシステムとマイクロカーネルの間にシステムサービスAPI(Application Programming Interface)を介在させてオペレーティングシステムを構成している。

【0057】

このようにすることにより、機能変更あるいは追加によるオペレーティングシステムの拡張性が向上するとともに、用途に対応する移植が容易になる。

また、マイクロカーネルの要素をネットワーク化された複数のコンピュータに分散配置することにより、分散オペレーティングシステムを実現することが容易になる。

【0058】

コンピュータはデスクトップ型あるいはノート型に代表されるパーソナルコンピュータ以外に、コンピュータ周辺機器、各種制御装置、通信機等に使用されている。その場合、各々の装置に適合するエンベデッド(組み込み)用の専用オペレーティングシステムとしてマン・マシン・インターフェースが重視される汎用のパーソナルコンピュータ用オペレーティングシステムと異なり、実行の早さが重視されるリアルタイムオペレーティングシステムが採用されている。

【0059】

当然のこととして組み込まれる装置毎に異なる専用のオペレーティングシステムの開発費用は大きい。そのため、最近ではエンベデッド（組み込み）用のリアルタイムオペレーティングシステムとしてパーソナルコンピュータ用の汎用オペレーティングシステムを転用することが提案されており、マイクロカーネルと組み合わされるサブシステムにエンベデッド用の固有のプログラムを配置することにより、組み込み用のリアルタイムオペレーティングシステムを得ることが行われている。

【0060】

オペレーティングシステムの大きな機能としてスケジューリングや割り込み処理等のタスク管理がある。

タスク管理に関して、オペレーティングシステムには大きく分けて同時に1つのタスク処理しか行わないシングルタスク方式と、同時に複数のタスク処理を行うマルチタスク方式があり、マルチタスク方式はさらにタスクの切り替えが処理されるタスクに依存するマルチタスク方式と、処理されるタスクに依存しないマルチタスク方式に区分される。

【0061】

これらの中、シングルタスク方式はMPUに1つのプロセスを割り当てそのプロセスが終了するまでMPUを解放しないものであり、ノンプリエンプティブマルチタスク方式はMPUを時分割して複数のプロセスに割り当てることができるが、実行中のプロセスがオペレーティングシステムに制御を戻さない限り他のプロセスは実行されないものであり、プリエンプティブマルチタスク方式はある時間間隔で実行中のプロセスに割り込みを行い、他のプロセスに強制的に制御を移すものである。

したがって、リアルタイムのマルチタスクはプリエンプティブ方式の場合にのみ可能である。

【0062】

コンピュータにおけるタスク管理はメモリやファイルなどのシステム資源を持つ単位であるプロセスに基づいて行われ、プロセスの管理はプロセスを細分化し

たCPU時間を割り当てる単位であるスレッドに基づいて行われる。なお、この場合システム資源は同一プロセス内の全てのスレッドで共有され、したがって一つのプロセス中にはシステム資源を共有する一つ以上のスレッドが存在することになる。

【0063】

マルチタスク方式で処理される各タスクには優先順位(Priority Spectrum)があり、一般的には32の段階に分けられる。この場合、割り込みを行わない通常のタスクは0-15段階に分けられるダイナミッククラス(Dynamic Classes)に区分され、割り込みを行うタスクは16-31段階に分けられるリアルタイムクラス(Real-Time Classes)に区分される。

【0064】

割り込み処理はタイムスライスと呼ばれる割り込み可能時間(通常10ms)を単位として行われ通常の割り込みは10msのタイムスライスで行われている。

このような状況において、最近リアルタイムスライスと呼ばれる割り込み可能時間が100 μ sであるタイムスライスが提案されたが、このリアルタイムスライスを利用すれば従来の10msの割り込みよりも優先して割り込みが可能である。

【0065】

図4に示された第3実施例では、ソフトウェアにより行われるコンピュータによる外部可変鍵方式暗号化/復号化処理及び暗号鍵の管理は、HALにおいてリアルタイムOSにより行われる。

この図において51はコンピュータ内のオペレーティングシステム、56はコンピュータからの出力を表示するディスプレイ装置、57は内蔵固定鍵方式暗号化/復号化ユニット、58はデジタルビデオディスク(DVD)RAMあるいはハードディスク等のデータ保存媒体、又はネットワーク等のデータ転送装置である。

【0066】

オペレーティングシステム51はユーザ領域であるオペレーティングシステムサービス部52、システムサービスAPI部53、非ユーザ領域であるカーネル

54部及びHAL55から構成され、システムサービスAPI部53はオペレーティングシステムサービス部52とカーネル部54の間に配置されて、オペレーティングシステムサービス部52とカーネル部54を仲介する役割を果たしており、HAL55はオペレーティングシステム50の最下層に配置され、ソフトウェアから見たハードウェアハードウェアの相異を吸収する役割を担っている。

【0067】

オペレーティングシステムサービス部52はアプリケーション59、サブシステム60及びセキュリティサブシステム61から構成され、カーネル部54は複数のマイクロカーネルモジュール62、64及びカーネル63から構成され、マイクロカーネルモジュール62はスケジューリング、割り込み等のタスク管理機能を有し、マイクロカーネルモジュール64はI/O管理機能を有する。

【0068】

I/O管理機能を有するマイクロカーネルモジュール64はI/Oマネージャ65、I/Oマネージャに管理されるディスクドライバ67、ネットワークドライバ68等のデバイスドライバ及びI/Oマネージャ65とディスクドライバ67、ネットワークドライバ68等のデバイスドライバとの間に必要に応じて挿入されるフィルタドライバ66から構成されている。

【0069】

コンピュータによる外部可変鍵方式暗号化／復号化処理はソフトウェアにより行われるが、第3実施例の場合には外部可変鍵方式暗号化／復号化処理はオペレーティングシステム51内のHAL55において他のタスクに優先して前に説明したリアルタイムOS(RTOS)により行われる。

【0070】

図2の第1実施例の場合と同様に、デジタル地上波放送、デジタルCATV放送、デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいはDVD、CD等のデジタル保存媒体により供給されるデジタルデータは、不正利用を防止するために暗号鍵K1を用いて暗号化されて、

$$C1 = E(M, K1)$$

供給され、供給された暗号化デジタルデータC1は暗号化デジタルデータC1と同

じ経路あるいは暗号化デジタルデータC1と異なる経路により鍵センタから提供された暗号鍵K1を用いてオペレーティングシステムサービス部52により復号され、

$$M = D(C1, K1)$$

復号化データMがディスプレイ装置56等に出力される。

【0071】

著作権主張がなされた復号化データMがデジタルビデオディスク(DVD)RAMあるいはハードディスク等の媒体に保存される場合、又はネットワークを経由して外部に転送される場合は、暗号化デジタルデータC1と同じ経路あるいは暗号化デジタルデータC1と異なる経路を経由して入手された外部可変鍵K2を用い、HAL55において復号化データMが強制的に再暗号化され、

$$C2 = E(M, K2) = E(D(C1, K1), K2)$$

さらに内蔵固定鍵方式暗号化／復号化装置57において再暗号化データC2がその内蔵固定鍵方式暗号化／復号化装置57に内蔵された固定暗号鍵K0を用いて再再暗号化され、

$$C2-0 = E(C2, K0) = E(E(D(C1, K1), K2), K0)$$

再再暗号化データC2-0として外部装置58に保存あるいは転送される。

【0072】

再再暗号化データC2-0が再利用される場合には、保存媒体から読み出されたあるいはネットワークを経由して転送された再暗号化データC2-0が内蔵固定鍵方式暗号化／復号化装置57において内蔵された固定暗号鍵K0を用いて再復号化され、

$$C2 = E(C2-0, K0) = D(E(E(D(C1, K1), K2), K0)$$

さらに外部可変鍵方式暗号化／復号化機能を有するHAL55において再復号化データC2が暗号化デジタルデータC1と同じ経路あるいは暗号化デジタルデータC1と異なる経路により鍵センターから入手した外部可変鍵K2を用いて復号化され、

$$M = D(C2, K2) = D(E(D(C1, K1), K2)$$

復号化データMがディスプレイ装置56等に出力される。

【0073】

リアルタイムOSは他の全てのタスクに優先して実行され、この第3実施例においてはリアルタイムOSがオペレーティングシステムのハードウェアとの接点であるHALにおいて実行されるから、デジタルデータの再暗号化が確実に行われ、復号化データMをそのまま外部装置58に保存あるいは転送することは不可能となる。また、内蔵固定鍵K0を用いて再暗号化する前に外部可変鍵K2を用いて再暗号化することにより、もし内蔵固定鍵が知られてしまった場合でもデータは外部可変鍵でも暗号化されているため、外部可変鍵を見いだして暗号化データの解読を行うことは極めて困難になる。

【0074】

また、外部可変鍵は初めに使用され、内蔵固定鍵が使用された後に、最後に使用されるため、暗号鍵の安全性が高く、かつ初めに使用されることにより、暗号化データを最も強力に支配することになる。

【0075】

図5に示された第4実施例では、ソフトウェアにより行われるコンピュータによる外部可変鍵方式暗号化／復号化処理は、カーネル部54内のI/O管理マイクロカーネルモジュール64に挿入されたフィルタドライバ66において行われる。

図6に示されたのは、フィルタドライバ66が挿入されたI/O管理マイクロカーネルモジュール64の構成である。

【0076】

フィルタドライバが挿入されていないI/O管理マイクロカーネルモジュールは上位階層から下位階層にファイルシステムドライバ69、中間ドライバ70、デバイスドライバ71が配置されており、必要に応じてファイルシステムドライバ69の上位階層あるいは中間ドライバ70とデバイスドライバ71との間にフィルタドライバ66Aあるいはフィルタドライバ66Bが挿入される。

【0077】

これらのフィルタドライバ66A及びフィルタドライバ66Bには再暗号化／再復号化処理及び暗号鍵の管理をさせることが可能であるため、この実施例にお

いは再暗号化／再復号化処理及び暗号鍵の管理をフィルタドライバ 66 A あるいはフィルタドライバ 66 B に実行させる。

【0078】

フィルタドライバはユーザが操作できるオペレーティングシステムサービス部 52 ではなくユーザが操作することができないカーネル部 54 に配置されている。しかし、オペレーティングシステムを使用するコンピュータに合わせて仕様を変更することが一般的に行われており、特に I/O 管理モジュールの内容を変更することは珍しいことではない。

【0079】

このことを利用して、第 4 実施例では再暗号化／再復号化処理及び暗号鍵の管理機能を有するモジュールをフィルタドライバ 66 A あるいはフィルタドライバ 66 B として I/O 管理モジュールに挿入する。

【0080】

図 2 の第 1 実施例の場合と同様に、デジタル地上波放送、デジタル CATV 放送、デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいは DVD、CD 等のデジタル保存媒体により供給されるデジタルデータは、不正利用を防止するために暗号鍵 K1 を用いて暗号化されて、

$$C1 = E(M, K1)$$

供給され、供給された暗号化デジタルデータ C1 は暗号化デジタルデータ C1 と同じ経路あるいは暗号化デジタルデータ C1 と異なる経路により鍵センタから提供された暗号鍵 K1 を用いてオペレーティングシステムサービス部 52 により復号され、

$$M = D(C1, K1)$$

復号化データ M がディスプレイ装置 56 等に出力される。

【0081】

著作権主張がなされた復号化データ M がデジタルビデオディスク (DVD) RAM あるいはハードディスク等の媒体に保存される場合、又はネットワークを経由して外部に転送される場合は、暗号化デジタルデータ C1 と同じ経路あるいは暗号化デジタルデータ C1 と異なる経路を経由して入手された外部可変鍵 K2 を用

い、フィルタドライバ 66A あるいは 66B において復号化データ M が強制的に再暗号化され、

$$C2 = E(M, K2) = E(D(C1, K1), K2)$$

さらに内蔵固定鍵方式暗号化／復号化装置 57 において再暗号化データ C2 がその内蔵固定鍵方式暗号化／復号化装置 57 に内蔵された固定暗号鍵 K0 を用いて再再暗号化され、

$$C2-0 = E(C2, K0) = E(E(D(C1, K1), K2), K0)$$

再再暗号化データ C2-0 として外部装置 58 に保存あるいは転送される。

【0082】

再再暗号化データ C2-0 が再利用される場合には、保存媒体から読み出されたあるいはネットワークを経由して転送された再暗号化データ C2-0 が内蔵固定鍵方式暗号化／復号化装置 57 において内蔵された固定暗号鍵 K0 を用いて再復号化され、

$$C2 = E(C2-0, K0) = D(E(E(D(C1, K1), K2), K0))$$

さらにフィルタドライバ 66A あるいは 66B において再復号化データ C2 が暗号化デジタルデータ C1 と同じ経路あるいは暗号化デジタルデータ C1 と異なる経路により鍵センターから入手した外部可変鍵 K2 を用いて復号化され、

$$M = D(C2, K2) = D(E(D(C1, K1), K2))$$

復号化データ M がディスプレイ装置 56 等に出力される。

【0083】

フィルタドライバは I/O 管理モジュールの一部として容易にオペレーションシステムのカーネル部に挿入することができ、このようにすることにより容易にオペレーションシステムに再暗号／再復号処理及び暗号鍵の管理機能を組み込むことができる。また、内蔵固定鍵 K0 を用いて再暗号化する前に外部可変鍵 K2 を用いて再暗号化することにより、もし内蔵固定鍵が知られてしまった場合でもデータは外部可変鍵でも暗号化されているため、外部可変鍵を見いだして暗号化データの解読を行うことは極めて困難になる。

【0084】

また、外部可変鍵は初めに使用され、内蔵固定鍵が使用された後に、最後に使

用されるため、暗号鍵の安全性が高く、かつ初めに使用されることにより、暗号化データを最も強力に支配することになる。

【0085】

図7に示された第5実施例では、ソフトウェアにより行われるコンピュータによる外部可変鍵方式暗号化／復号化処理及び暗号鍵管理は、オペレーティングシステム51内のI/O管理マイクロカーネルモジュール64に含まれるディスクドライバ57及びネットワークドライバ68において行われる。

【0086】

図6で説明したように、I/O管理マイクロカーネルモジュールは上位階層から下位階層にファイルシステムドライバ69、中間ドライバ70、デバイスドライバ71が配置されており、その最下層に位置するデバイスドライバ71でも外部可変鍵方式暗号化／復号化処理及び暗号鍵管理を行うことができる。

【0087】

図2の第1実施例の場合と同様に、デジタル地上波放送、デジタルCATV放送、デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいはDVD、CD等のデジタル保存媒体により供給されるデジタルデータは、不正利用を防止するために暗号鍵K1を用いて暗号化されて、

$$C1 = E(M, K1)$$

供給され、供給された暗号化デジタルデータC1は暗号化デジタルデータC1と同じ経路あるいは暗号化デジタルデータC1と異なる経路により鍵センタから提供された暗号鍵K1を用いてオペレーティングシステムサービス部52により復号され、

$$M = D(C1, K1)$$

復号化データMがディスプレイ装置56等に出力される。

【0088】

著作権主張がなされた復号化データMがデジタルビデオディスク(DVD)RAMあるいはハードディスク等の媒体に保存される場合、又はネットワークを経由して外部に転送される場合は、暗号化デジタルデータC1と同じ経路あるいは暗号化デジタルデータC1と異なる経路を経由して入手された外部可変鍵K2を用

い、ディスクドライバ67及びネットワークドライバ68であるデバイスドライバ71において復号化データMが強制的に再暗号化され、

$$C2 = E(M, K2) = E(D(C1, K1), K2)$$

さらに内蔵固定鍵方式暗号化／復号化装置57において再暗号化データC2がその内蔵固定鍵方式暗号化／復号化装置57に内蔵された固定暗号鍵K0を用いて再再暗号化され、

$$C2-0 = E(C2, K0) = E(E(D(C1, K1), K2), K0)$$

再再暗号化データC2-0として外部装置58に保存あるいは転送される。

【0089】

再再暗号化データC2-0が再利用される場合には、保存媒体から読み出されたあるいはネットワークを経由して転送された再暗号化データC2-0が内蔵固定鍵方式暗号化／復号化装置57において内蔵された固定暗号鍵K0を用いて再復号化され、

$$C2 = E(C2-0, K0) = D(E(E(D(C1, K1), K2), K0)$$

さらにディスクドライバ67及びネットワークドライバ68であるデバイスドライバ71において再復号化データC2が暗号化デジタルデータC1と同じ経路あるいは暗号化デジタルデータC1と異なる経路により鍵センターから入手した外部可変鍵K2を用いて復号化され、

$$M = D(C2, K2) = D(E(D(C1, K1), K2)$$

復号化データMがディスプレイ装置56等に出力される。

【0090】

デバイスドライバは、オペレーティングシステムを使用するコンピュータに合わせてあるいは対象となるデバイスが改良されたような場合に仕様を変更することが極く一般的に行われている。

【0091】

このようなデバイスドライバに再暗号／再復号処理及び暗号鍵の管理機能を組み込むことによりオペレーションシステムのカーネル部にこれらの機能を容易に組み込むことができる。また、内蔵固定鍵K0を用いて再暗号化する前に外部可変鍵K2を用いて再暗号化することにより、もし内蔵固定鍵が知られてしまっ

た場合でもデータは外部可変鍵でも暗号化されているため、外部可変鍵を見いだして暗号化データの解読を行うことは極めて困難になる。

【0092】

また、外部可変鍵は初めに使用され、内蔵固定鍵が使用された後に、最後に使用されるため、暗号鍵の安全性が高く、かつ初めに使用されることにより、暗号化データを最も強力に支配することになる。

【0093】

このようにデジタルデータの再暗号化／再復号化を行うためにはそのデジタルデータの保存あるいは転送が制限されていることを識別する符号をデジタルデータに付加しておく必要がある。そして、デジタルデータが加工されることなく保存あるいは転送される場合には、これまでに述べてきた再暗号化／再復号化方法及び装置によって、デジタルデータの不正な利用を防止することができる。

【0094】

しかし、デジタルデータに加工が行われた場合には保存あるいは転送が制限されていることを識別する符号が失われる可能性がある。

【0095】

そのような場合には、全てのデータをその装置に固有の暗号鍵（マスターキー）を用いて再暗号化／再復号化するようにすればよい。

このようにすることにより、カット&ペースト等の方法により加工されたデジタルデータの場合でも再暗号化／再復号化することにより不正な利用を防止することができる。

【0096】

なお、その場合マスターキーを用いて再暗号化／再復号化するデジタルデータは保存あるいは転送が制限されていることを識別する符号が付されていないものに限定し、保存あるいは転送が制限されていることを識別する符号が付されているデジタルデータの場合にはこれまでに述べた実施例で説明した方法及び装置により再暗号化／再復号化するようにしてもよい。

【0097】

外部可変鍵K2は何度も繰り返して使用されると知られてしまう危険性がある

。そのような場合には、特開平 8-185448 号公報に述べられたように暗号化使用された暗号鍵 K2 は廃棄され、復号に必要なときには、再度鍵センタから入手するようにすることが適切である。

【0098】

また、安全のため K1, K2, K0 は異なる暗号アルゴリズムによるものを使用しても良い。

【図面の簡単な説明】

【図 1】

従来提案されているセットトップボックスの概要構成図。

【図 2】

セットトップボックスに適用したの本発明第 1 実施例の概要構成図。

【図 3】

セットトップボックスに適用したの本発明第 2 実施例の概要構成図。

【図 4】

パーソナルコンピュータを用いた装置に適用した本発明第 3 実施例の概要構成図。

【図 5】

パーソナルコンピュータを用いた装置に適用した本発明第 4 実施例の概要構成図。

【図 6】

本発明第 4 実施例の詳細な説明図。

【図 7】

パーソナルコンピュータを用いた装置に適用した本発明第 5 実施例の概要構成図。

【符号の説明】

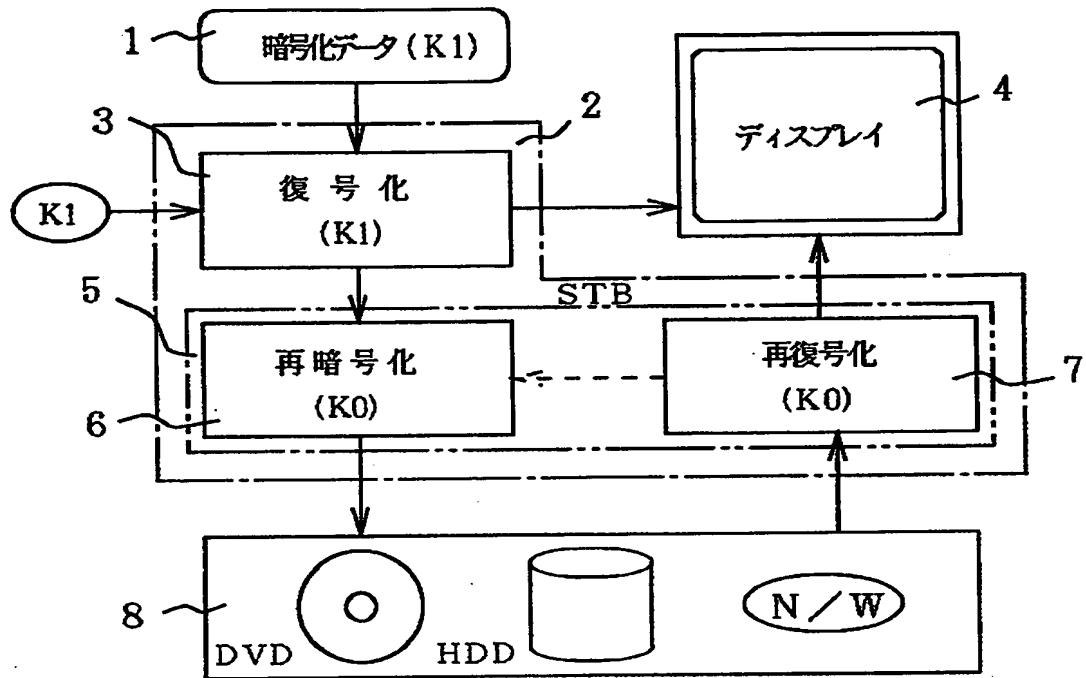
-
- | | |
|-----------|------------|
| 1, 11, 31 | 暗号化データ |
| 2, 12, 32 | セットトップボックス |
| 3, 13, 33 | 復号化ユニット |
| 4, 14, 34 | ディスプレイ装置 |

- 5, 15, 35 内蔵固定鍵方式暗号化／復号化ユニット
- 6, 20, 36, 41 再暗号化ユニット
- 7, 17 再復号化ユニット
- 8, 18 外部装置
- 16, 40 再再暗号化ユニット
- 19, 39 外部可変鍵方式暗号化／復号化ユニット
- 21, 37 再再復暗号化ユニット
- 35, 57 内蔵固定鍵方式暗号化／復号化ユニット
- 41 外部可変鍵方式暗号化／復号化ユニット
- 51 オペレーティングシステム
- 52 オペレーティングシステムサービス部
- 53 システムサービスAPI部
- 54 カーネル部
- 55 HAL
- 56 ディスプレイ装置
- 58 データ保存媒体・データ転送装置
- 59 アプリケーション
- 60 サブシステム
- 61 セキュリティサブシステム
- 62, 64 マイクロカーネルモジュール
- 63 カーネル
- 65 I/Oマネージャ
- 66, 66A, 66B フィルタドライバ
- 67 ディスクドライバ
- 68 ネットワークドライバ

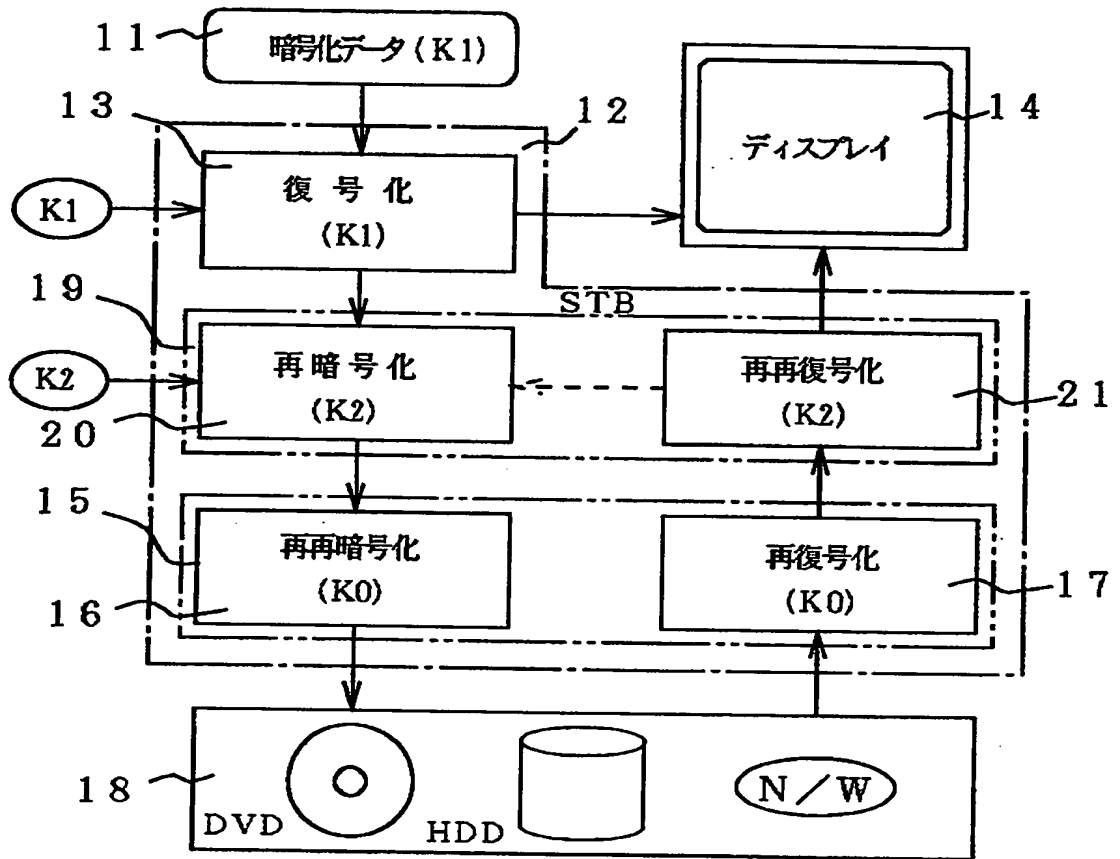
【書類名】

図面

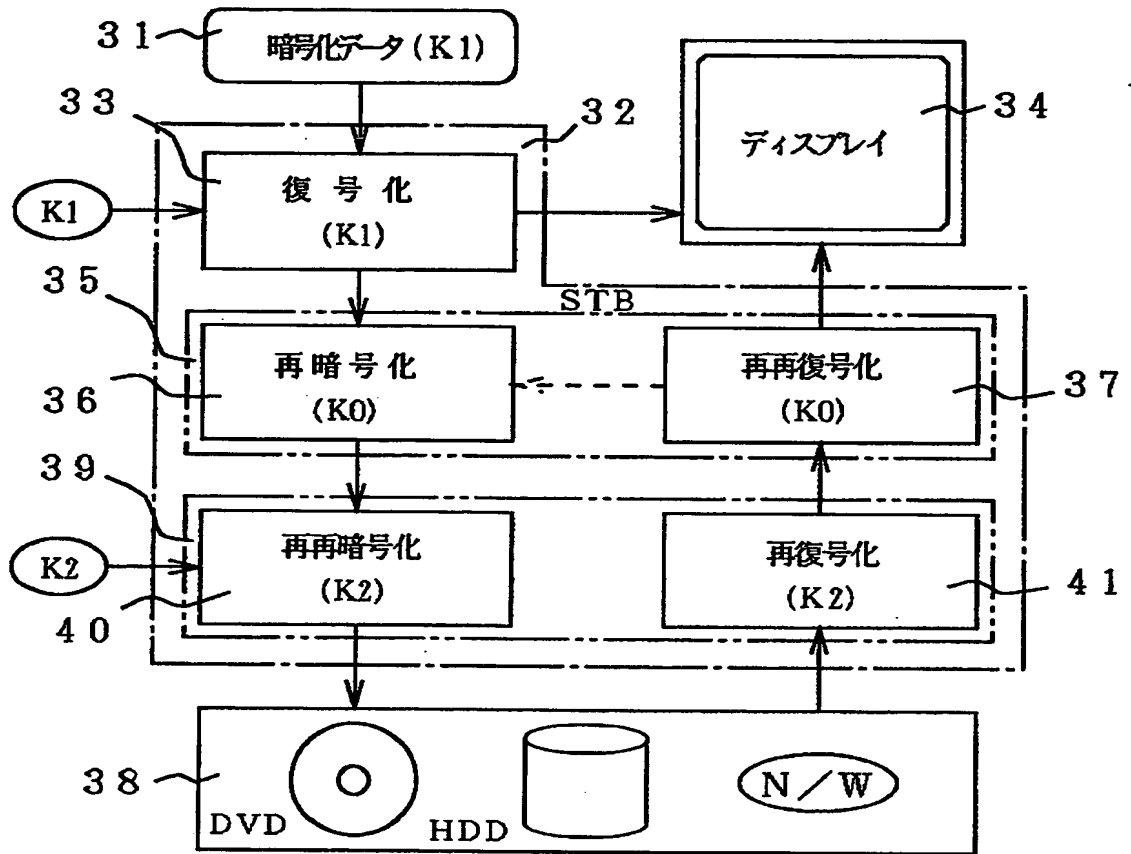
【図 1】



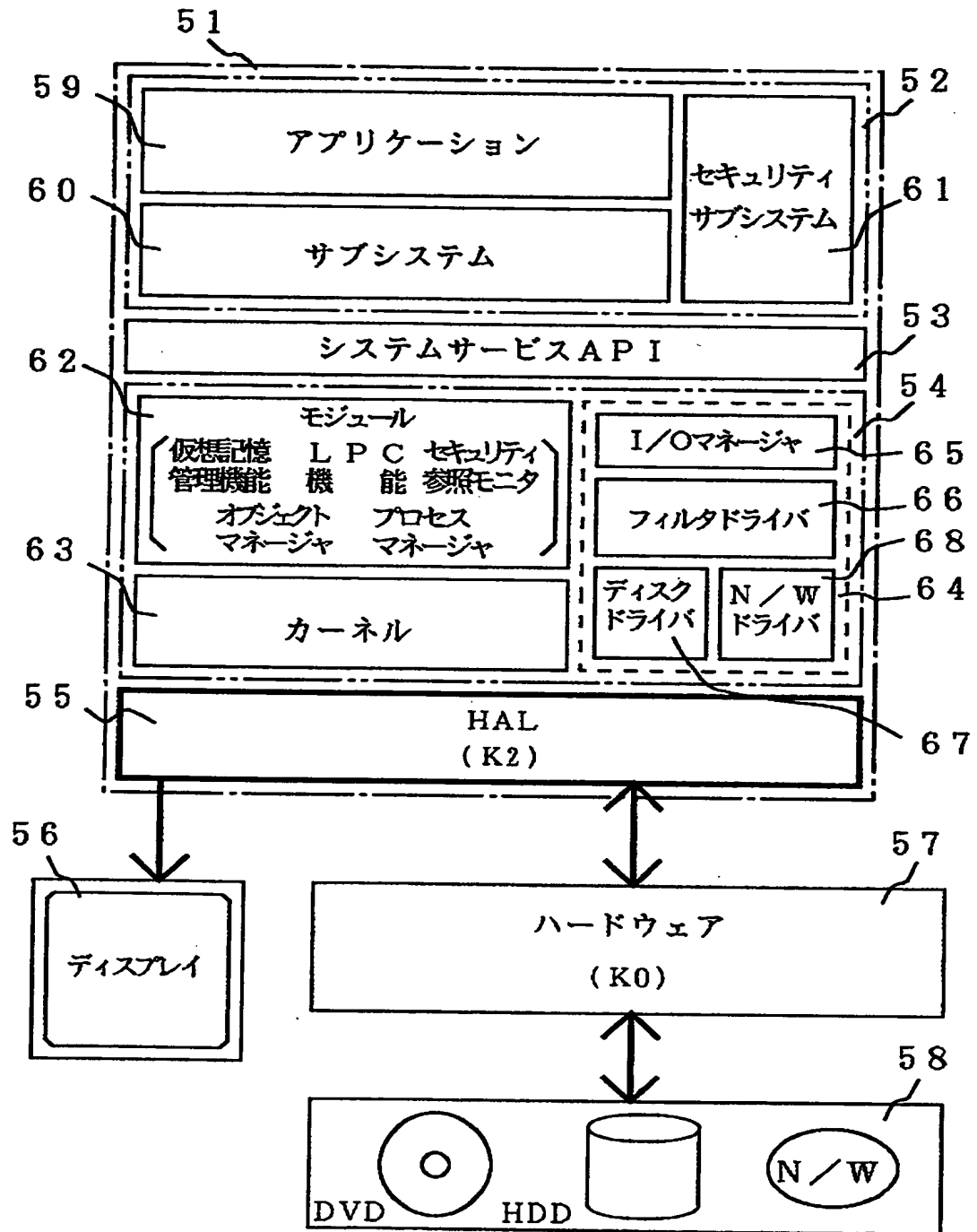
【図 2】



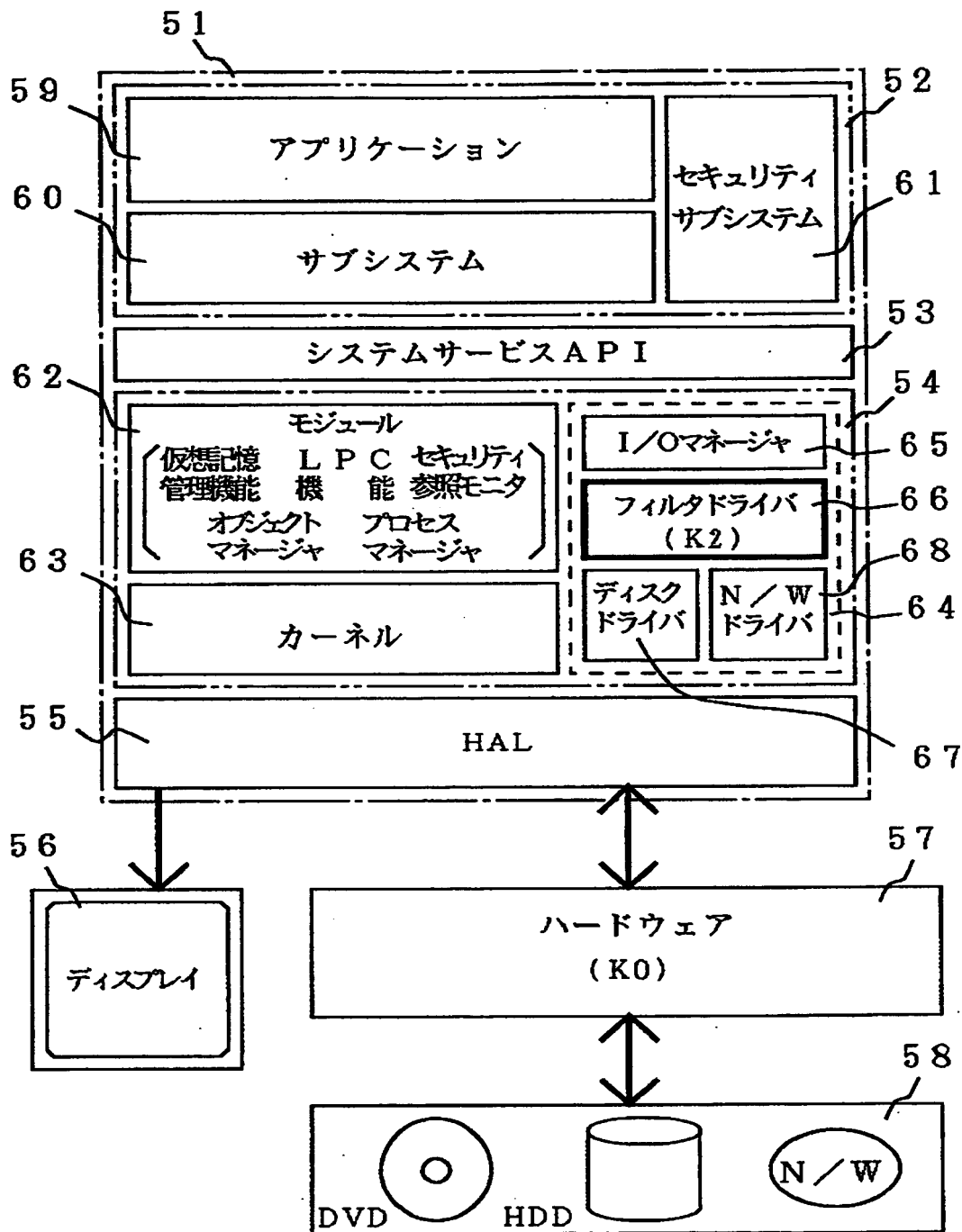
【図 3】



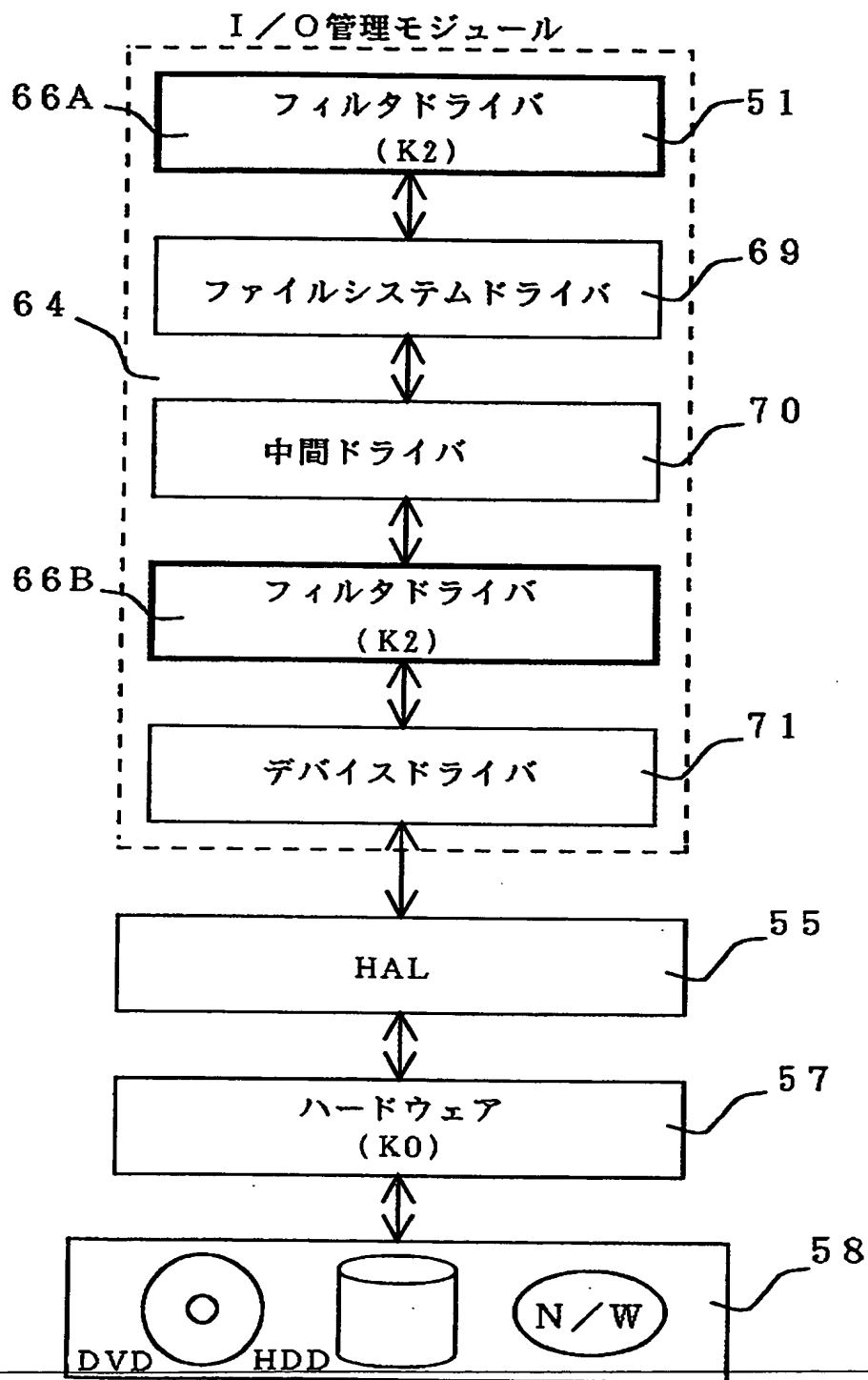
【図4】



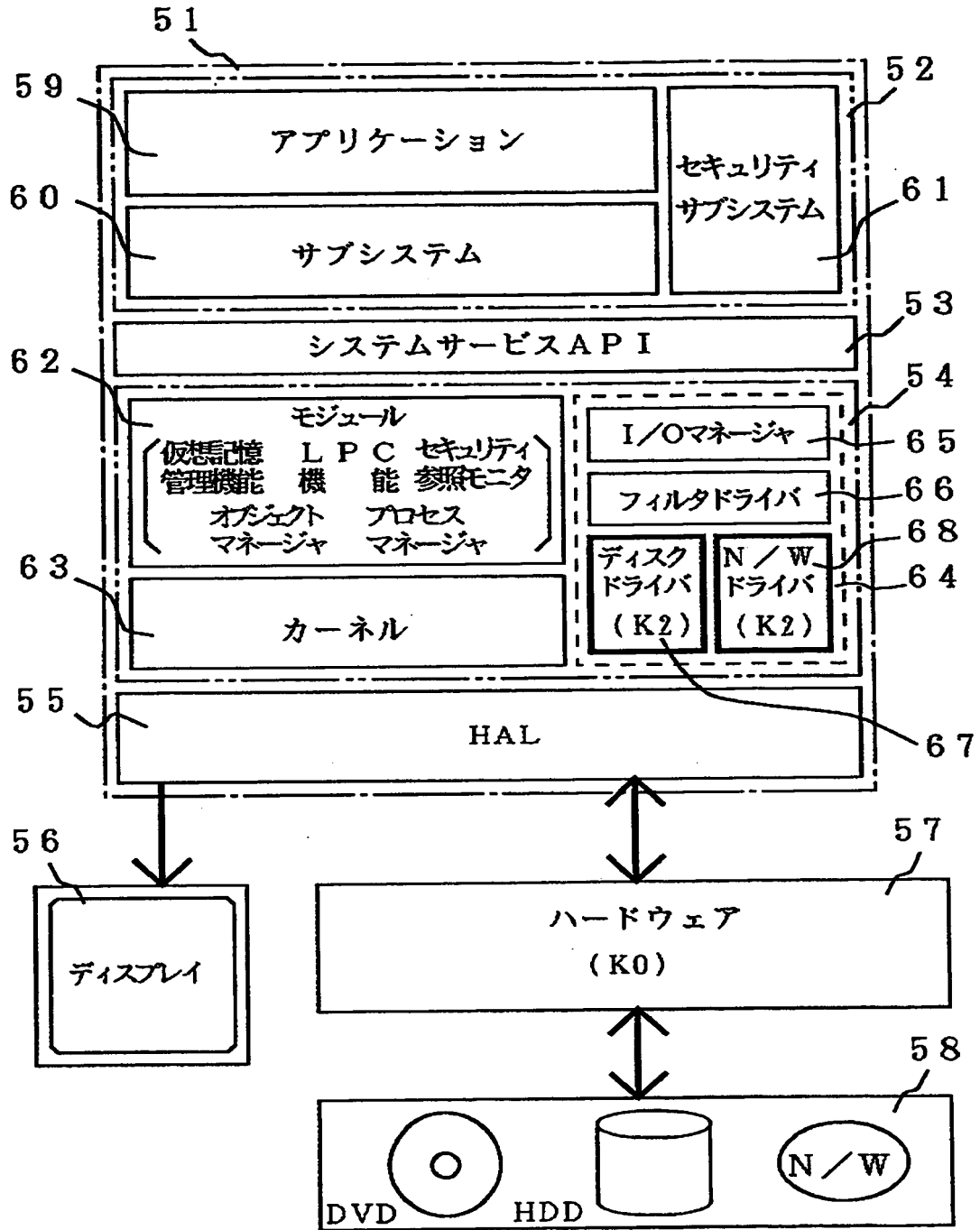
【図5】



【図6】



【図 7】



【書類名】 要約書

【要約】

【課題】 確実に再暗号化する方法及び装置を提供する。

【解決手段】 内蔵固定鍵を用いる再暗号化に加えて外部の可変鍵を用いて2重に再暗号化する。暗号鍵の使用順には、初めに可変鍵を用い次に固定鍵を用いる場合と、初めに固定鍵を用い次に可変鍵を用いる場合とがある。実施形態としてはソフトウェアによる場合とハードウェアによる場合があり、さらにソフトウェアとハードウェアの組み合わせがある。ハードウェアとしてはデジタルビデオに向けて開発された内蔵固定鍵を用いるハードウェアが利用可能である。ソフトウェアによる場合プログラム及び使用される鍵の安全性を保全するためにユーザが利用することができないカーネル部以下の領域で暗号化／復号化を行う。具体的にはI/Oマネージャ内のフィルタドライバ、ディスクドライバ・ネットワークドライバであるデバイスドライバ、HALを利用するRTOSで暗号化／復号化を行う。フィルタドライバはファイルシステムドライバを挟んで2つあるがどちらも利用可能であり、さらには両方を利用することも可能である。

【選択図】 図2

【書類名】

職権訂正データ

【訂正書類】

特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】

000005979

【住所又は居所】

東京都千代田区丸の内2丁目6番3号

【氏名又は名称】

三菱商事株式会社

【代理人】

申請人

【識別番号】

100099379

【住所又は居所】

東京都千代田区神田美土代町7番地 クボビル

【氏名又は名称】

南條 眞一郎

出 願 人 履 歴 情 報

識別番号 [000005979]

1. 変更年月日 1990年 8月13日

[変更理由] 新規登録

住 所 東京都千代田区丸の内2丁目6番3号
氏 名 三菱商事株式会社

THIS PAGE BLANK (USPTO)

=This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)